قسم الامن السيبراني

Department of Cyber Security

Subject: Virtualization & Data Security

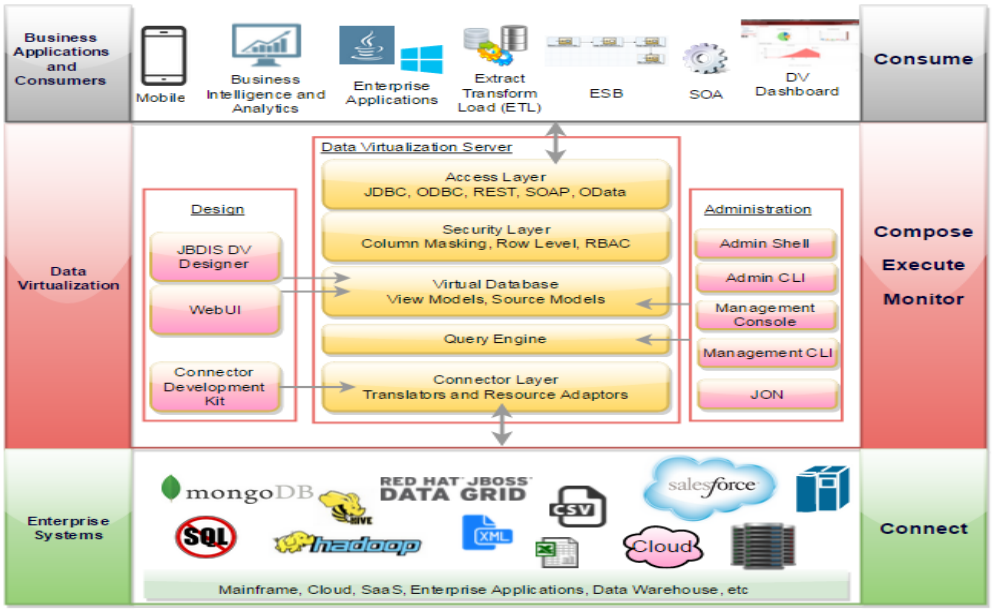
Class: Third stage

Lecture: (5)

Lecturer: Msc :Najwan thaeer ali

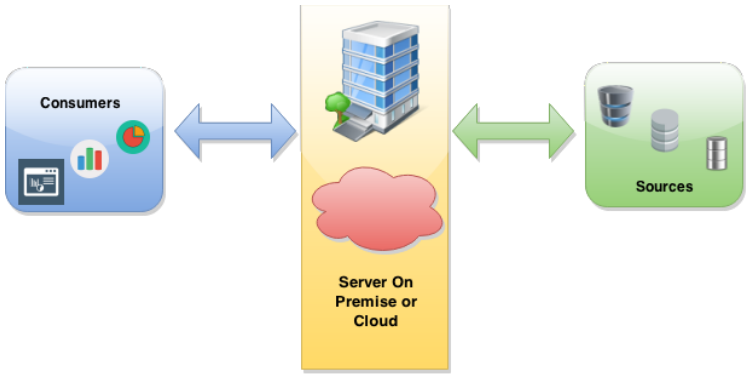
What Is Nested Virtualization? How Does It Work?

Nested virtualization :is the ability to run a hypervisor *inside* a virtual machine (VM), so you can create and manage other VMs within that VM. This is done by safely exposing hardware-assisted virtualization extensions (like Intel VT-x/AMD-V and EPT/NPT) from the physical host to the guest, allowing the guest operating system to function as a hypervisor itself.



If you're exploring modern lab setups, cloud-native development, or complex QA pipelines, you'll likely encounter nested virtualization sooner or later. In simple terms, it lets one VM behave like a physical server that can host additional virtual machines — ideal for training,

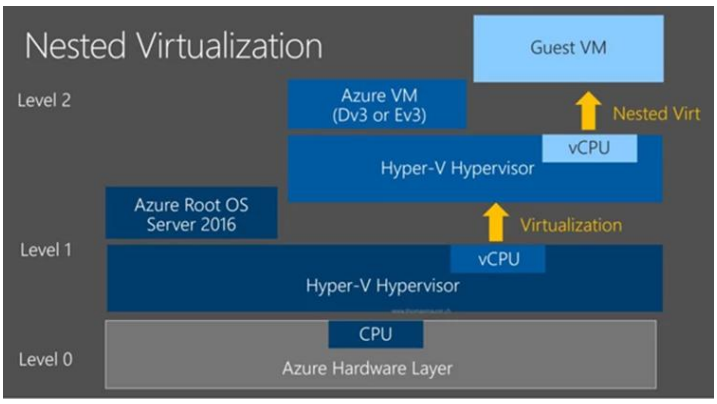
testing, and running multi-layered environments *without additional hardware*.



What Is Nested Virtualization?

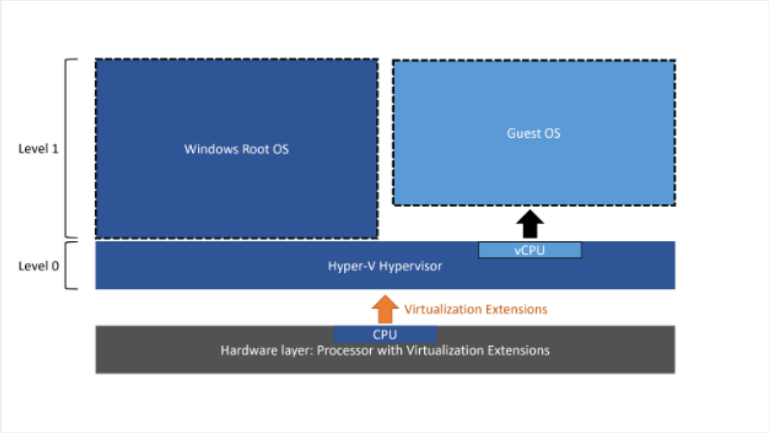
Nested virtualization allows a guest VM to run its own hypervisor. In industry terminology:

- **L0** = the hypervisor running on the physical host
- **L1** = the hypervisor running inside a VM
- **L2** = the VMs created by the L1 hypervisor



How Nested Virtualization Works

Modern CPUs provide virtualization features (such as Intel VT-x and AMD-V) and second-level address translation (EPT/NPT) for efficient memory management. In a nested setup, the host hypervisor (L0) passes these capabilities to the L1 guest so that the L1 hypervisor can create and run L2 VMs without fully emulating a CPU.



Common Use Cases

Nested virtualization is useful for:

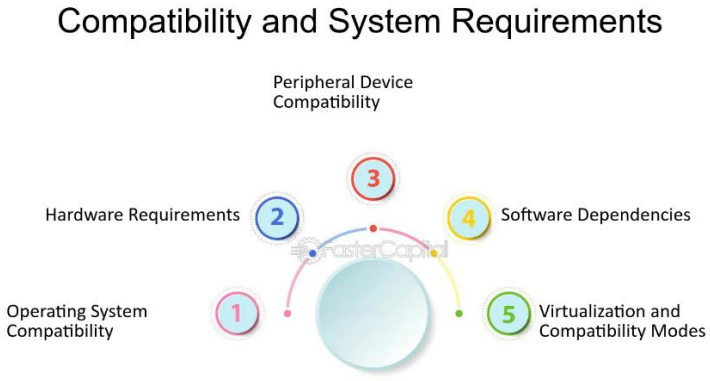
- **Education and training labs:** running full virtualization labs without dedicated physical hardware
- **Development/QA environments:** testing hypervisor-dependent software or CI pipelines on virtual machines
- **Cloud-native demonstrations:** simulating complex production environments with Kubernetes, OpenStack, etc.

- **Network Function Virtualization (NFV):** chaining virtual network services across layers
- **Migration testing:** validating migration paths without touching production systems

Requirements and Compatibility

To use nested virtualization:

- CPUs must support virtualization extensions (Intel VT-x with EPT or AMD-V with NPT)
- The host hypervisor (like KVM, Hyper-V, or VMware ESXi) must support nesting
- The nested guest hypervisor can be Windows with Hyper-V or Linux with KVM
- Sufficient CPU cores, RAM, and storage I/O are needed because nested VMs multiply resource demands



Advantages and Limitations

Advantages:

- Consolidates complex lab environments on a single physical server
- Flexible testing without extra hardware
- Faster cloning and snapshotting of full hypervisor stacks
- Cost-effective for training and pre-production validation

Limitations:

- Increased overhead and latency compared to running directly on the host
- Requires modern hardware and current firmware
- Troubleshooting is more complex due to multiple layers
- Not ideal for high-latency sensitive production workloads

Security Considerations

- Nested layers increase the attack surface
- Strict isolation policies and updated firmware/hypervisors are essential
- Disable nested virtualization when not needed to reduce risk

Conclusion

Nested virtualization lets you run a hypervisor *inside* a VM to build full lab and testing environments on a single server. By exposing hardware virtualization features (VT-x/AMD-V and EPT/NPT) to the guest, you can create multi-layered stacks that mimic real production setups. Planning capacity, following best practices, and working with knowledgeable providers helps ensure correct deployment.